

METHOD AND APPARATUS FOR OBSERVING NETWORK-SAFETY ENSURING POLICY IN PUBLIC KEY CRYPTOGRAPH SYSTEM

Publication number: JP5216411 (A)

Also published as:

Publication date: 1993-08-27

JP2552061 (B2)

Inventor(s): SUTEFUAN EMU MATEIASU; DONARUDO BII JYONSON; AN BUI
RII; UIRAMU SHII MAASTEIN; ROSUTEISUROU PURAIMATSUKU;
UIRAMU ESU ROORANDO; JYON DEI UIRUKINSU +

US5164968 (A)

EP0539726 (A2)

EP0539726 (A3)

EP0539726 (B1)

Applicant(s): IBM +

more >>

Classification:
- international: G06F21/00; G09C1/00; H04L9/08; H04L9/32; G06F1/00;
G06F21/00; G09C1/00; H04L9/08; H04L9/32; G06F1/00; (IPC1-
7): G09C1/00

- European: G06F21/00N1D1; H04L9/08C; H04L9/32

Application number: JP19920261293 19920930

Priority number(s): US19910786227 19911031

Abstract of JP 5216411 (A)

PURPOSE: To provide an improvement method for key management in a public key cipher system.

CONSTITUTION: A device A continues to faithfully execute a safety guaranteeing policy instructed by an authorization center 10 as long as the public key PUMa of the device A is authorized. When the device A changes the operation from the ciphered limit of an old constitution vector by the loading of a new constitution vector for instance, the participation to the network of the device A is denied. In order to achieve the execution of the network safety guaranteeing policy instructed by the authorization center 10, it is required to make the authorization center 10 recognize that the device A is constituted of an authenticated present constitution vector at the point of time when the device A requests the authorization of the public key PUMa.



Data supplied from the **espacenet** database — Worldwide